Compliance Component

DEFINITION

Name	Firewall Environments
Description	Firewall Environment is a term used to describe the set of systems and components that are involved in providing or supporting the complete firewall functionality at a given point on a network. Firewall Environments are made up of firewall devices and associated systems and applications designed to work together.
Rationale	The Firewall Environment provides adequate protection for the organization's networks while minimizing complexity and management.
Benefits	• Creates defense in depth with layer security • Coordinates security between firewalls, intrusion detection systems, and other network security devices • Restricts connectivity between networks • Provides a buffer zone for transactions with outside parties • Secures remote access

ASSOCIATED ARCHITECTURE LEVELS

List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Secure Gateways and Firewalls
List Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	Firewall Environments may consist of: • Firewall(s) • Demilitarized Zones (DMZs) • Virtual Private Networks (VPNs) • Intranets • Extranets • Hubs and switches • Intrusion Detection Systems (IDS) • Domain Name Server (DNS) • Server placement A simple firewall environment may consist of a packet filter firewall and nothing else. In a more complex and secure environment, it may consist of several firewalls, proxies, and specific topologies for supporting the systems and security.

Building Firewall Environments

- A firewall shall be used between any agency-controlled equipment and equipment not controlled by the agency such as that owned by other agencies, contractors, business partners or public service providers.
- The environment configuration should be simple. The more simple the firewall solution, the more secure it will likely be and the easier to manage. Complexity in design and function can lead to errors in configuration.
- Do not make firewalls out of equipment not intended to be firewalls. For example, network switches used as firewalls can be susceptible to attack.
- A router should not be used as a firewall unless special firewall software is installed on it.
- Create defense in depth by creating layers of security as opposed to one layer. Where several firewalls can be used, they should be. Where routers can be configured to provide some access control or filtering, they should be.
- Internal firewalls should be used to protect important systems from internal threats. Examples include internal web and email servers, and financial systems.

DMZs

- A DMZ is created by network switches that sit between an internal and external firewall, or between an internal firewall and a boundary router. Agencies should not use just one firewall to create a DMZ since the firewall would be subject to service degradation during denial of service attacks.
- DMZs shall serve as connection points for systems that require or support external connectivity, or between internal systems with different levels of access control.
- Agencies shall place remote access servers and external VPN endpoints within DMZs.

VPNs

- External VPN appliances shall be installed in the DMZ. Placing it behind the firewall would require that encrypted VPN traffic be passed outbound through the firewall, and the firewall would then be unable to inspect the inbound or outbound traffic, or perform access control or logging.

Intranets

- An intranet is a network that employs HTTP for internal information dissemination.
- An intranet must be behind the firewall.
- An internal firewall should be used to separate intranets.

Extranets

- An extranet is two or more networks that are joined via the Internet.
- The agency shall implement a firewall, controlled by the agency, on its side of the extranet.

Hubs and Switches

- Network hubs shall not be used to build DMZs or firewall environments.
- Network switches should be used for implementing DMZs and firewall environments.
- Network switches shall not be used to provide any firewall or traffic isolation capability outside of a firewall environment.

IDS

- Host-based intrusion detection systems shall be placed on all systems in the DMZ and any internal systems that can be accessed by external entities.
- Network-based intrusion detection systems shall be placed on the private side of the firewall.
- Network-based intrusion detection systems should also be placed on the public side of the firewall and may be in the DMZ.

DNS

- Internal Domain Name Servers (DNS) shall be kept separate from external domain name servers. This practice, known as split DNS, ensures that private internal systems are never identified to external organizations.
- Access to external DNS shall only be allowed through port 53 (the standard port for DNS).
- Agencies should configure computers to use specific DNS servers by IP address, and should not allow blind zone transfers.

Firewall Failover Strategies

- If the firewall environment does not have redundancy, the connection must be automatically severed if the firewall fails.
- Redundancy and failover services should be provided for firewall environments. This can be done using:
  - specially designed network switches that shift all traffic over to a backup firewall in the event of a failure,
  - a customized "heartbeat" mechanism that typically involves a network interface to notify the backup firewall of the primary firewall’s functionality, or
  - a manually initiated backup firewall.
- Network switches that provide load balancing and failover capabilities allow seamless failover and, in many cases, established sessions through the firewall are not impacted by a production system failure. The network switch-based failover

solution is generally the most expensive solution.

- Heartbeat-based solutions almost always lose established sessions traversing the production firewall in the transition from production to backup resources.
- A manually initiated backup firewall is the least desirable, but also the least expensive.

Placement of Servers in Firewall Environments

- Where to place servers in a firewall environment depends on many factors. The following guidelines can be used to make the determination:
  - Place internal servers behind internal firewalls as their sensitivity and access require.
  - Isolate servers such that attacks on the servers do not impair the rest of the network.
- Externally accessible servers shall be placed in the DMZ. The boundary router can provide some access control and filtering for the servers, and the main firewall can restrict connections from the servers to internal systems, which could occur if the servers are penetrated.
- External VPN and Dial-In Servers shall be placed in the DMZ. This enables outbound traffic to be encrypted after it has been filtered (e.g., by an HTTP proxy) and allows inbound traffic to be decrypted and filtered by the firewall.
- Internally accessible web servers, email servers, and directory servers should be placed in the DMZ. This provides defense in depth protection from external threats, and well as protection from internal threats. Web mail servers shall be set to only accept SMTP connections through the firewall.
- To access web mail from an external network, an SSL proxy shall run on the main firewall. Using a web browser, external users authenticate to the main firewall. The main firewall forwards the SSL connection to the internal proxy/email server for a second authentication. This solution prevents direct external access to the mail server, yet still permits external access through the firewall.

Document Source Reference #			
Standard Organization			
Name	NIST SP 800-41, Guideline for Firewalls and Firewall Policy	*Website*	www.csrc.nist.gov/publications/Intpubs
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST)	*Website*	http://csrc.nist.gov/
Contact Information			

KEYWORDS				
List all Keywords	Contractor, partner, DMZ, VPN, DNS, extranet, intranet, heartbeat, failover, failsafe, blind zone, IDS, packet filter, dial-in			
COMPONENT CLASSIFICATION				
Provide the Classification	□ *Emerging*	☒ *Current*	□ *Twilight*	□ *Sunset*
Rationale for Component Classification				
Document the Rationale for Component Classification				
Conditional Use Restrictions				
Document the Conditional Use Restrictions				
Migration Strategy				
Document the Migration Strategy				
Impact Position Statement				
Document the Position Statement on Impact				
CURRENT STATUS				
Provide the Current Status)	□ *In Development*	□ *Under Review*	☒ *Approved*	□ *Rejected*
AUDIT TRAIL				
Creation Date	06/08/2004	*Date Accepted / Rejected*	06/08/2004	
Reason for Rejection				
Last Date Reviewed		*Last Date Updated*		
Reason for Update				